

REMARKS/ARGUMENTS

This Reply is being filed in response to the third non-final Official Action of April 20, 2006, in which all of the pending claims, namely Claims 1-18, stand rejected under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent Application Publication No. 2003/0033528 to Ozog et al. Initially, Applicant would like to thank the Examiner for taking the time to conduct a telephone interview with Applicant's undersigned attorney about the Official Action, and in particular Ozog as interpreted in the Official Action. As explained below, Applicant respectfully submits that the claimed invention is patentably distinct from Ozog, and accordingly traverses the rejection of the claims as being anticipated thereby. In view of the following remarks, Applicant respectfully requests reconsideration and allowance of all of the pending claims of the present application.

A. The Ozog Publication

Ozog discloses a method for an issuer, *B*, to grant a "mandate" to a beneficiary, *A*, allowing the beneficiary to obtain information or services on behalf of the issuer from a third party. As shown in FIG. 4 and disclosed in Ozog, issuer *B* asks beneficiary *A* for *A*'s public key. Beneficiary *A*, after receiving a public key certificate from any certification authority (CA), sends issuer *B* its public key certificate (certificate CA(X)). Issuer *B* then requests a beneficiary public key certificate (certificate VCA(B)) from a mandate authority based on beneficiary *A*'s public key certificate (certificate CA(X)), with beneficiary *A* as the owner and issuer *B* as a virtual CA (VCA). Finally, issuer *B* sends, to beneficiary *A*, a mandate that *A* may then use to obtain information or services on behalf of the issuer. The mandate includes an issuer certified reference (certificate provided to the issuer from a service provider), a beneficiary certified reference (beneficiary certificate / certificate VCA(B)), the date of issuance, and other general validation rules.

Following issuance of the mandate by the issuer *B* to the beneficiary *A*, the beneficiary may request proprietary information of the issuer *B* from a service provider by appending the mandate (digitally signed by issuer *B*) in a request (digitally signed by beneficiary *A*). Upon receipt of the request, the service provider can validate the mandate based on the issuer certified

reference (certificate provided to the issuer by the service provider) and the mandate's digital signature of *B*. The service provider can then validate the request based on the beneficiary certified reference (beneficiary certificate / certificate VCA(*B*)) and the request's digital signature of *A*.

B. The Claimed Invention

As previously explained, in accordance with one aspect of the claimed invention of the present application, as currently recited by independent Claim 1, a system is provided that includes a terminal, a secondary certification authority (CA), a tertiary CA and a server. As recited, the terminal is included within an organization including a plurality of terminals, where at least one terminal has at least one characteristic and is at one or more of a plurality of positions within an organization. The organization includes a plurality of secondary CA's capable of issuing role certificates to respective groups of terminals of the organization, and includes a plurality of tertiary CA's capable of issuing permission certificates to respective sub-groups of terminals of the organization. In this regard, the secondary CA is capable of providing at least one role certificate to the terminal based upon the position of the terminal within the organization. The tertiary CA, on the other hand, is capable of providing at least one permission certificate to the terminal based upon the characteristics of the respective terminal. Thus, the server is capable of authenticating the terminal based upon an identity certificate, the role certificate and the permission certificate of the terminal to thereby determine whether to grant the terminal access to at least one resource of the server.

C. Distinctions between the Ozog Publication and the Claimed Invention

Applicant initially notes that based on the interpretation of Ozog given by the Official Action, Applicant presumes that the Official Action interprets the beneficiary / requestor (person A) of Ozog as corresponding to the terminal of the claimed invention. For purposes of this Reply, Applicant takes this correspondence as given (but expressly does not admit its accuracy). As described above, then, Ozog and the claimed invention both generally relate to use of certificates to authenticate a computing device. In contrast to independent Claim 1, however,

Ozog does not teach or suggest (i) a secondary CA providing role certificate(s) to a terminal based upon position(s) of the terminal within an organization; (ii) a tertiary CA providing permission certificate(s) to the terminal based upon characteristic(s) of the terminal at a position in the organization; or (iii) a server authenticating the terminal based upon an identity certificate, the role certificate(s) and the permission certificate(s).

1. Providing Role Certificate(s)

The third Official Action interprets the issuer / grantor certified reference and the VCA(B) certificate (beneficiary certificate) of Ozog as corresponding to role certificate(s) as recited by the claimed invention. As disclosed by Ozog and explained above, the issuer / grantor certified reference and VCA(B) certificate (beneficiary certificate / beneficiary certified reference) are included within a mandate, which is provided from an issuer to a beneficiary for use by the beneficiary to access proprietary information of the issuer at a service provider. However, Ozog does not teach or suggest that the respective certificates are provided to a beneficiary (terminal) based upon position(s) of the beneficiary within an organization, similar to the role certificate(s) of the claimed invention. In fact, Ozog does not teach or suggest any basis for the provision of these respective certificates other than to authenticate the beneficiary to access resources of the issuer at a service provider. Even considering this basis, however, the certificates are provided to the beneficiary irrespective of the beneficiary's position in an organization.

Properly interpreted, as explained above, the issuer / grantor certified reference is issued by a service provider to the issuer *B* to bind the issuer *B* to a public key. By digitally signing the subsequent mandate utilizing a corresponding private key, then, the service provider can verify the mandate as being from a valid issuer. The VCA(B) certificate (beneficiary certificate / beneficiary certified reference), on the other hand, is issued by a virtual certification authority (CA) of issuer *B* to the beneficiary *A* to bind the beneficiary to a public key. The public key bound to the beneficiary *A* is the same public key bound to beneficiary *A* via certificate CA(X), but whereas certificate CA(X) is issued by a CA not having a trust relationship with the service provider, certificate VCA(B) is issued a virtual CA of *B*, which does have a trust relationship

with the service provider. Thus, by digitally signing the request utilizing a corresponding private key, the service provider can verify that the request originated from the entity to which the certificate in the mandate (i.e., the VCA(B) certificate / beneficiary certificate / beneficiary certified reference) was issued. Thus, instead of being provided to the beneficiary B based upon position(s) of the beneficiary within an organization, similar to the role certificate(s) of the claimed invention, the respective certificates are provided solely on the basis of the beneficiary A being authorized to access information of issuer B.

2. *Providing Permission Certificate(s)*

For the recited feature of providing permission certificate(s) to the terminal (aforementioned feature (ii)), the Official Action cites to the mandate disclosed by Ozog. As indicated above, Ozog discloses that an issuer / grantor B can authorize a beneficiary / requestor A to access information of the issuer / grantor B on a service provider via a mandate provided by the issuer / grantor B. Again, Ozog does not teach or suggest that the mandate is provided to the beneficiary A based upon based upon characteristic(s) of the beneficiary A at a position in the organization, similar to the permission certificate(s) of the claimed invention. Rather, the mandate is provided to authorize the beneficiary A to access information of the issuer / grantor B, irrespective of any characteristic(s) of the beneficiary A.

Applicant does note that Ozog discloses implementation of its system in the context of a wireless operator issuer authorizing access to services of the operator to a corporation beneficiary. As disclosed, the wireless operator issues a mandate to the corporation for employees, or for specific employees (i.e., specific type of employee), of the corporation. One could therefore argue that the corporation in this instance corresponds to an organization, and that being a specific type of employee in the corporation corresponds to being at a position in the organization. Under this argument, one could then argue that Ozog discloses providing a mandate to beneficiary employees of the corporation at a respective position in the corporation (i.e., being a specific type of employee). Even in this instance, however, Ozog does not teach or suggest that the mandate is provided based upon characteristic(s) of the employees at their

respective position in the organization, similar to the permission certificate(s) of the claimed invention.

3. *Authenticating a Terminal Based on Identity, Role and Permission Certificates*

Finally, for the recited feature of authenticating the terminal based upon an identity certificate, the role certificate(s) and the permission certificate(s) (aforementioned feature (iii)), the Official Action cites the passage of Ozog directed to a service provider providing access control for information of an issuer requested by a beneficiary having a mandate from the issuer. Under this interpretation, the Official Action cites the original public key certificate of the beneficiary *A* issued by CA(X), i.e., certificate CA(X). Applicant respectfully submits, however, that the service provider of Ozog does not, in fact, authenticate the beneficiary *A* based upon certificate CA(X). In this regard, as disclosed by Ozog, one option for the service provider to authenticate the beneficiary *A* would be for the beneficiary *A* to simply append its public key certificate, i.e., certificate CA(X), to the request from beneficiary *A*. Ozog, paragraph [0062]. Ozog explicitly discloses that this option is not practical, however, since it would require the service provider to have a trust relationship with CA(X). Thus, instead of authenticating the beneficiary based upon a certificate from a CA with which the service provider does not have a trust relationship, the service provider of Ozog authenticates the beneficiary based upon the beneficiary certificate from the virtual CA of issuer B (i.e., VCA(B) certificate – alleged to correspond to a role certificate), with which the service provider does have a trust relationship.

Applicants therefore respectfully submit that the service provider of Ozog authenticates a beneficiary based upon two certificates, namely, a issuer / grantor certificate (issuer / grantor certified reference) and a beneficiary certificate (beneficiary certified reference / VCA(B) certificate). The claimed invention, on the other hand, recites authenticating a terminal based upon at least three certificates, namely, an identity certificate, role certificate(s) and permission certificate(s).

Accordingly, Applicant respectfully submits that the claimed invention of independent Claim 1, and by dependency Claims 2-6, is patentably distinct from Ozog. Applicant also

Appl. No.: 10/749,042
Amdt. dated 07/20/2006
Reply to Official Action of April 20, 2006

respectfully submits that independent Claims 7 and 13 recite subject matter similar to independent Claim 1. For example, independent Claims 7 and 13 recite providing a role certificate and a permission certificate, and authenticating a terminal based upon those certificates as well as an identity certificate. Accordingly, Applicant respectfully submits that the claimed invention of independent Claims 7 and 13, and by dependency Claims 8-12 and 14-18, is patentably distinct from Ozog for at least the same reasons given above with respect to independent Claim 1. Applicant therefore respectfully submits that the rejection of Claims 1-18 under 35 U.S.C. § 102(a) as being anticipated by Ozog is overcome.

Appl. No.: 10/749,042
Amdt. dated 07/20/2006
Reply to Official Action of April 20, 2006

CONCLUSION

In view of the remarks presented above, Applicant respectfully submits that the present application is in condition for allowance. As such, the issuance of a Notice of Allowance is therefore respectfully requested. In order to expedite the examination of the present application, the Examiner is encouraged to contact Applicant's undersigned attorney in order to resolve any remaining issues.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,



Andrew T. Spence
Registration No. 45,699

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

ELECTRONICALLY FILED USING THE EFS-WEB ELECTRONIC FILING SYSTEM OF THE UNITED STATES PATENT & TRADEMARK OFFICE ON JULY 20, 2006.